Assessing the Threat:

Past and Future

James Halverson & Gary Ackerman

WINS Workshop: Evolving Security Threats and Advanced Security Technologies

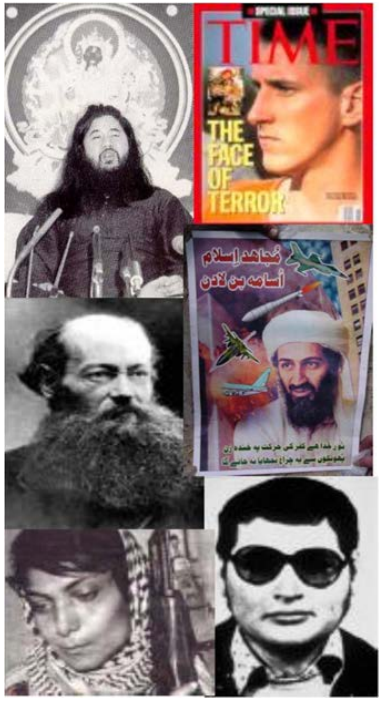
March 19, 2018

Introduction

- Critical infrastructure has long been a prime target for non-state actors who aim to deal blows, instrumental or expressive, against state power
- The nuclear sector is no exception, but is a special case
  - Powerful place in the popular imagination
  - Must worry about not only disruption and damage but also theft
  - A threat anywhere can be problematic everywhere
- Uniquely attractive to actors with objectives that span beyond borders

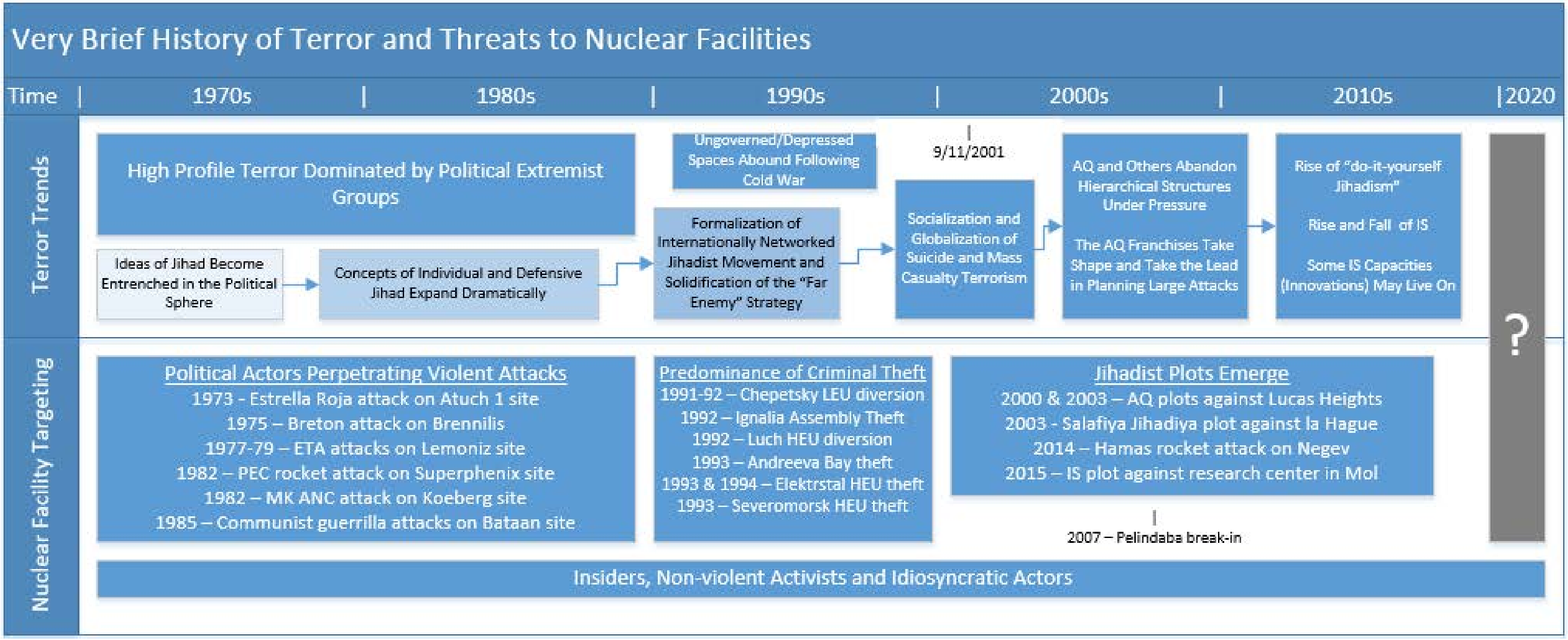
Motives for Targeting Critical Infrastructure

- **Expressive Motives**
  - Undercutting state authority or prestige
- **Instrumental Motives**
  - Mass casualties
  - Economic and Socio-political disruption
  - Status relative to competitors/Prestige
- The Role of Serendipity/Opportunity
- Actual motives typically a combination
- Motivation/Intention must coincide with Capability/Opportunity for successful attack
  - Analysis and forecasting complicated by the difficulty measuring motivation, the need to unpack Capability/Opportunity and the interdependence of these factors



Motives for Specifically Targeting Nuclear

- **Expressive Motives**
  - Undercutting state authority or prestige with an international audience
  - Apocalyptic / millenarian worldview
  - Techno-fetishism
- **Instrumental Motives**
  - Exert profound psychological impact internationally
    - Adjusting for target’s discomfort threshold (public habituation)
  - Intensified disruption due to radioactive release or fear thereof
  - Status relative to internal and external rivals / Prestige (the “innovators”)
  - Profit (historically tied very closely to opportunity)
- Serendipity/Opportunity
  - Insiders
  - Vulnerable facilities



Very Brief History of Terror and Threats to Nuclear Facilities

Time | 1970s | 1980s | 1990s | 2000s | 2010s | 2020

Terror Trends

High Profile Terror Dominated by Political Extremist Groups

Ideas of Jihad Become Entrenched in the Political Sphere

Concepts of Individual and Defensive Jihad Expand Dramatically

Ungoverned/Depressed Spaces Abound Following Cold War

Formalization of Internationally Networked Jihadist Movement and Solidification of the "Far Enemy" Strategy

9/11/2001

Socialization and Globalization of Suicide and Mass Casualty Terrorism

AQ and Others Abandon Hierarchical Structures Under Pressure

The AQ Franchises Take Shape and Take the Lead in Planning Large Attacks

Rise of "do-it-yourself Jihadism"

Rise and Fall of IS

Some IS Capacities (Innovations) May Live On

?

Nuclear Facility Targeting

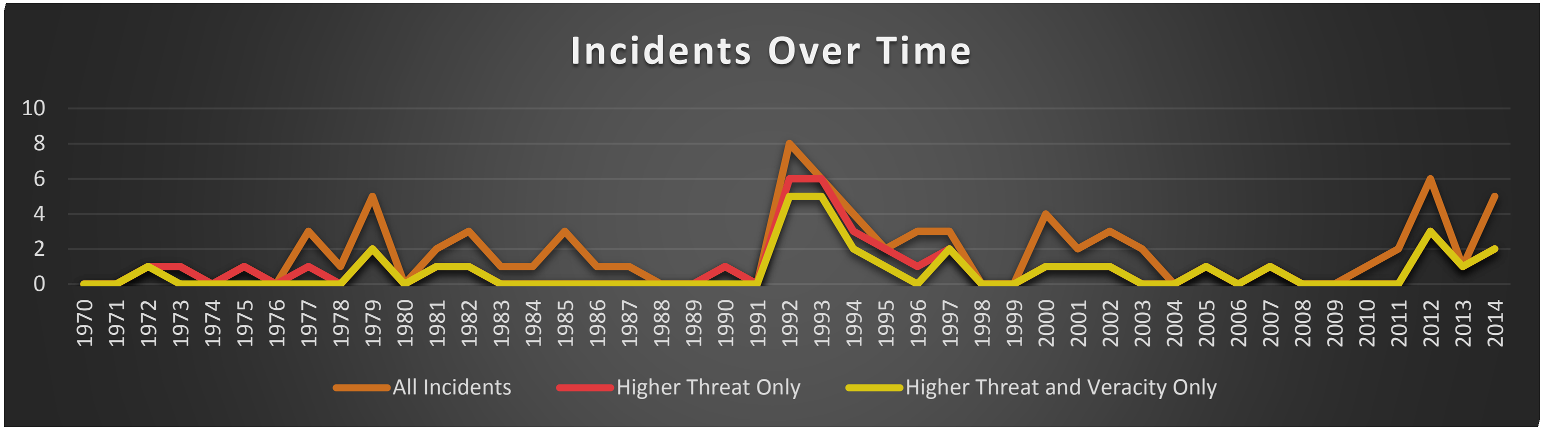
Political Actors Perpetrating Violent Attacks
1973 - Estrella Roja attack on Atuch 1 site
1975 – Breton attack on Brennilis
1977-79 – ETA attacks on Lemoniz site
1982 – PEC rocket attack on Superphenix site
1982 – MK ANC attack on Koeberg site
1985 – Communist guerrilla attacks on Bataan site

Predominance of Criminal Theft
1991-92 – Chepetsky LEU diversion
1992 – Ignalia Assembly Theft
1992 – Luch HEU diversion
1993 – Andreeva Bay theft
1993 & 1994 – Elektrstal HEU theft
1993 – Severomorsk HEU theft

Jihadist Plots Emerge
2000 & 2003 – AQ plots against Lucas Heights
2003 - Salafiya Jihadiya plot against la Hague
2014 – Hamas rocket attack on Negev
2015 – IS plot against research center in Mol

2007 – Pelindaba break-in

Insiders, Non-violent Activists and Idiosyncratic Actors



Incidents Over Time

What’s In the Trends?

- Correlations
  - Occurrences of nuclear facility attacks correlate strongly, on a national level, with the presence of guerrilla warfare and to a lesser degree with anti-government demonstrations
  - Attacks on other types of critical infrastructure not found to be a strong indicator

What’s In the Trends?

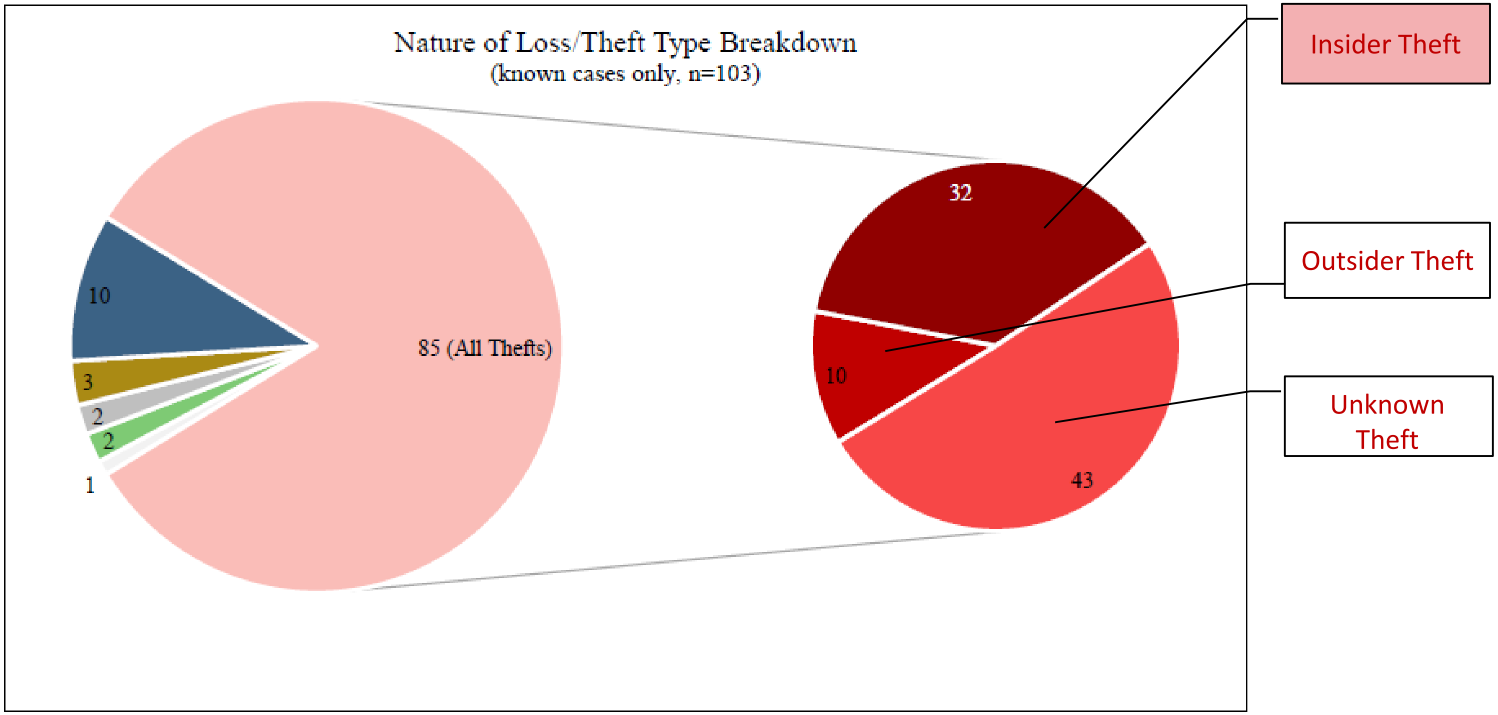
- Event Characteristics
  - Insiders prevalent and dangerous
  - Criminal and Revolutionary/Separatist actors most successful in sophisticated breaches, but no interest in inducing RN hazards
  - Successful attacks and infiltrations virtually never occur outside of perpetrators’ familiar areas of operations (Kinshasa and Pelindaba potential exceptions)
    - Though jihadists the first to really try
  - Most breaches decidedly low-tech, though stand-off/aerial weapons can prove problematic

Insiders

- Among 80 breaches of highly secured nuclear facilities (41 high-threat) at least 25% of all breaches and 44% - 52% of high-threat breaches involved insiders.
  - 35% - 63% of breaches that achieved their ostensible goals involved insiders
  - Initial survey of expanded data suggests this trend is even stronger
- Extremist organizations aware of the utility of insiders
  - 1990s: Aum Shinrikyo – Recruits hundreds of scientists with sensitive knowledge
  - 2001: Bashir-ud-din Mahmood & Abdul Majid – PAEC scientists meet with UBL
  - 2009: Adlene Hicheur – CERN scientist in contact with al Qa'ida
  - 2015: Yassim Salhi – Lyon chemical plant
  - 2016: el Bakraoui brothers – Surveilled prominent SCK CEN employee

Insider Theft

- Among facilities known to have lost any sort of uranium or plutonium since 1990 (including ore and depleted uranium)
  - Theft is the most reported mode (83%)
  - Insiders involved in most cases where this could be determined (76%)



What’s In the Trends?

- Event Characteristics
  - Insiders prevalent and dangerous
  - Criminal and Revolutionary/Separatist actors most successful in sophisticated breaches (thefts and attacks), but no prior interest in inducing RN hazards
  - Successful attacks and infiltrations virtually never occur outside of perpetrators familiar areas of operations (Kinshasa and Pelindaba potential exceptions)
    - Though jihadists the first to really try
  - Most breaches decidedly low-tech, though stand-off/aerial weapons prove problematic

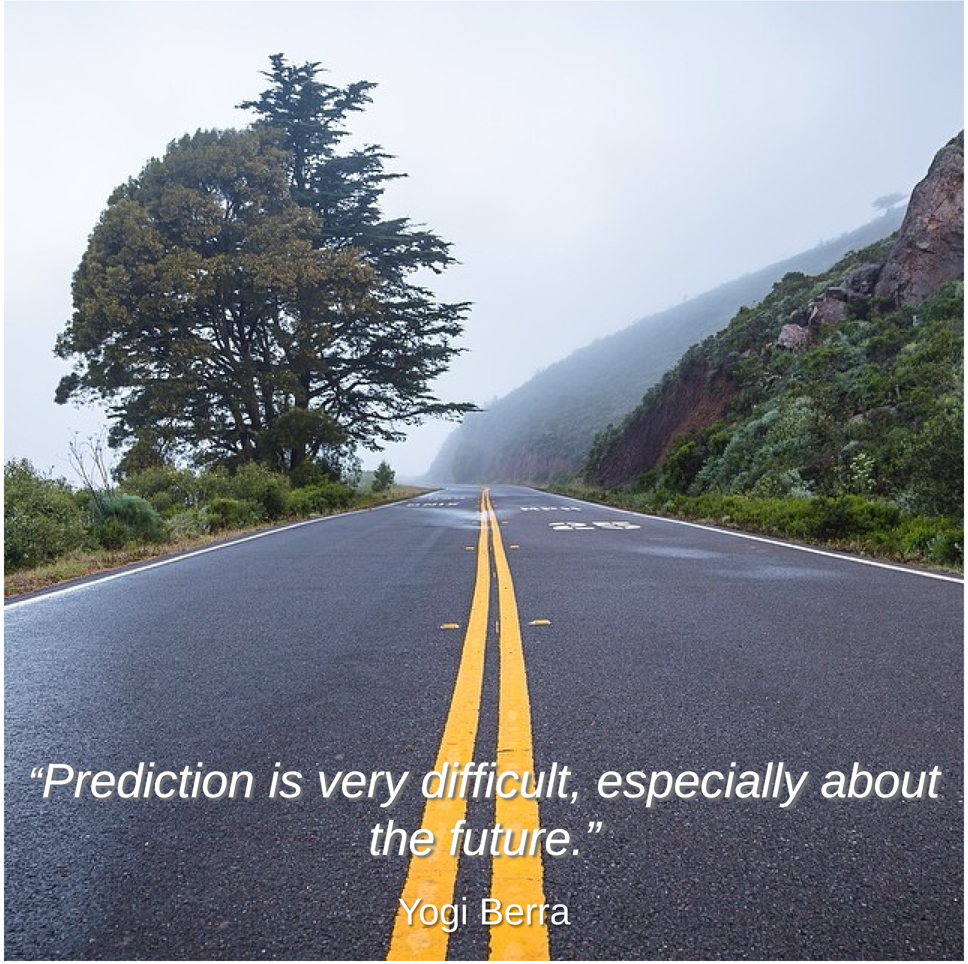
What’s In the Trends?

- Event Characteristics
  - Insiders prevalent and dangerous
  - Criminal and Revolutionary/Separatist actors most successful in sophisticated breaches, but no prior interest in inducing RN hazards
  - Successful attacks and infiltrations virtually never occur outside of perpetrators’ familiar areas of operations (Kinshasa and Pelindaba potential exceptions)
    - Though jihadists the first to really try
  - Most breaches decidedly low-tech, though stand-off/aerial weapons prove problematic

What’s In the Trends?

- Event Characteristics
  - Insiders prevalent and dangerous
  - Criminal and Revolutionary/Separatist actors most successful in sophisticated breaches, but no prior interest in inducing RN hazards
  - Successful attacks and infiltrations virtually never occur outside of perpetrators’ familiar areas of operations (Kinshasa and Pelindaba potential exceptions)
    - Though jihadists the first to really try
  - Most breaches decidedly low-tech, though stand-off/aerial weapons prove problematic

What Lies Ahead?



"Prediction is very difficult, especially about the future."

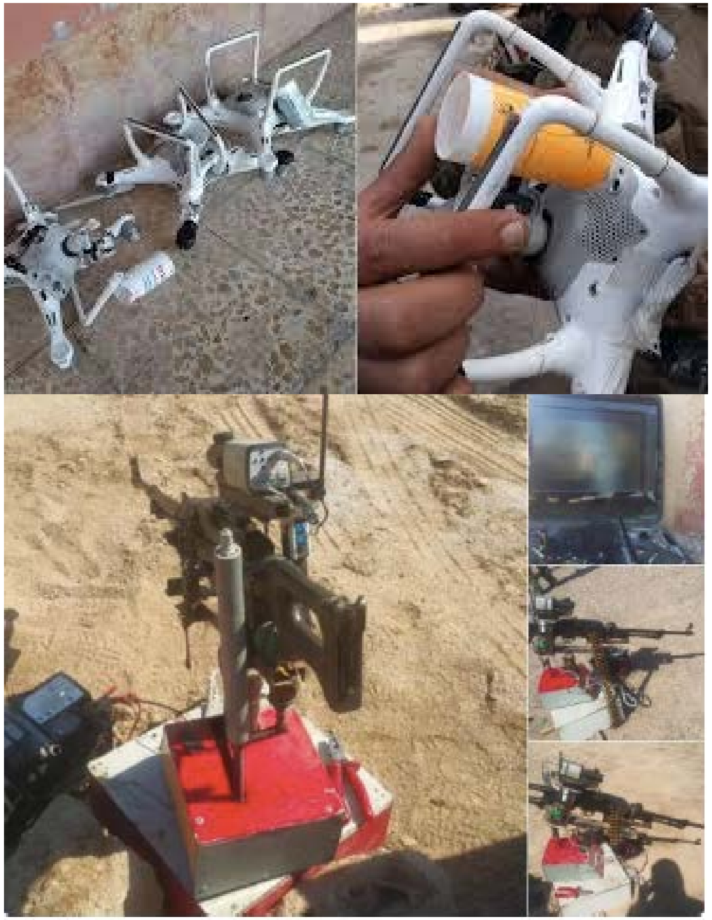
Yogi Berra

Evolution of the Threat Actors

- Salafi jihadists remain the prime concern due to a combination of capability and intention to perpetrate <u>violence with an audience</u>
  - Movement poised to atomize and fill spaces where rule of law is lacking – less capable but more numerous contingents looking to make their mark
  - Failure of the caliphate leaves the door open for “far-enemy” strategies to return to favor
  - History instructs that the near targets (Pakistan, UAE, research reactors in North Africa) face greater threat
  - Can learn from nationalist and criminal exploits

Syria an “Incubator of Innovation”

- Drone bombs
- Remote gun turrets
- Chemical weapons (mustard production)

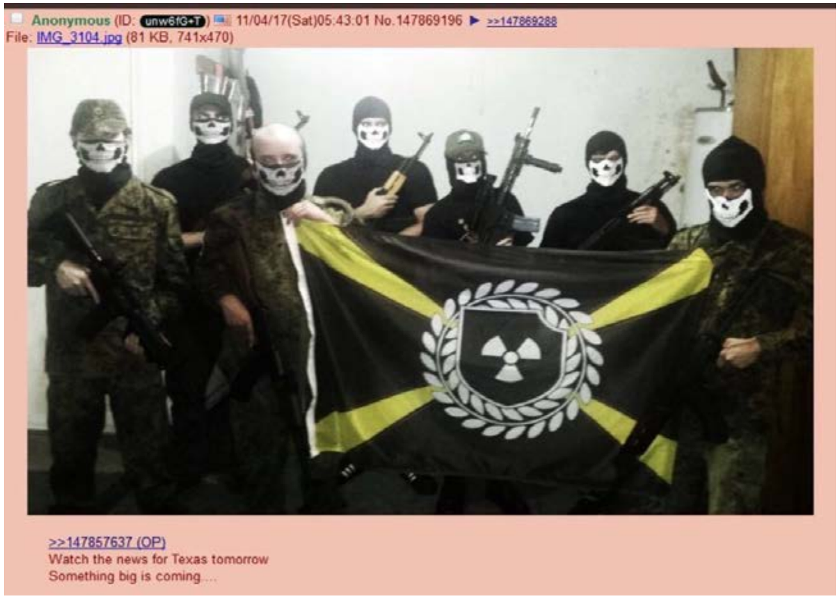


Evolution of the Threat Actors

- Nationalists, separatists and revolutionaries remain a real threat
  - Tensions persist after 2003 and 2006 Baloch separatist attacks on Dera Ghazi Khan PAEC facility
  - HAMAS bridges adversary types (Dimona attack)
  - Unrest in East Ukraine abuts spaces rich in nuclear infrastructure
  - Houthi rebels recently claimed attack on UAE reactor site
  - Ethno-nationalists in India, Uyghur separatists in China

Evolution of the Threat Actors

- Fetishizing of nuclear within new western nationalist boom?
  - “Atomwaffen” group, active in more that 20 states, plotted against Turkey River NPP and leader possessed thorium and americium samples



□ Anonymous (ID: unw6fG+T) 11/04/17(Sat)05:43:01 No.147869196 ▶ >>147869288
File: IMG_3104.jpg (81 KB, 741x470)

>>147857637 (OP)
Watch the news for Texas tomorrow
Something big is coming....

Evolution of External Drivers

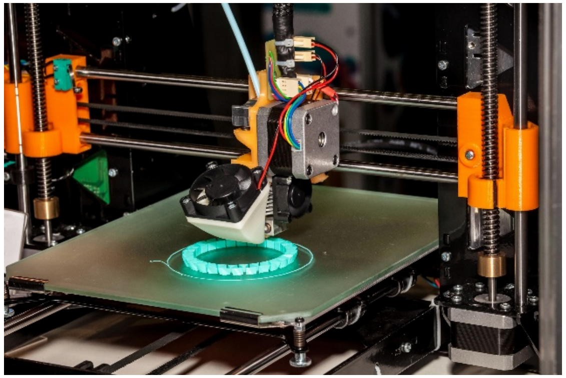
- Large-scale nuclear security disruptions loom
  - Some appear relatively certain for the near-term
    - Political attention and funding lacking
    - International cooperative appetites soured
  - Others sure to come but over longer spans
    - Climate change
    - Unemployment (of the highly educated)
  - Others still are stochastic and sudden
    - Economic collapse
    - Large-scale armed conflict
    - Natural Disaster
    - Pandemics

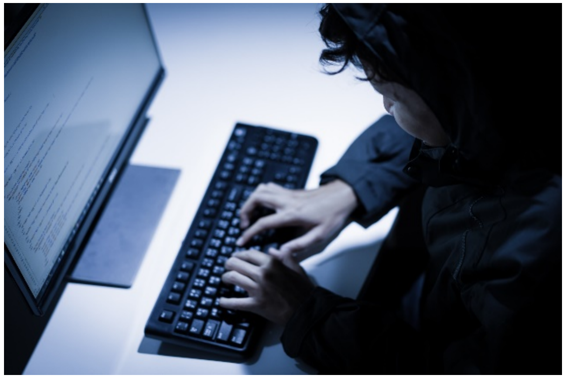
Evolution of Industry Drivers

- Energy competition from natural gas and renewables
  - Security budgets further embattled?
- Facilities finding the fighting
  - Nuclear ambitions throughout the developing world
  - History indicates that new projects in unstable spaces are at singular risk
- Interim spent fuel storage crowding
- New design learning curve

Technology an Ever More Powerful Driver

“The future is already here — it's just not very evenly distributed” - William Gibson





“The IQ level required for a single individual to destroy the world decreases by one point every year”
– Eliezer Yudkowsky

Evolution of External Drivers (Tech.)

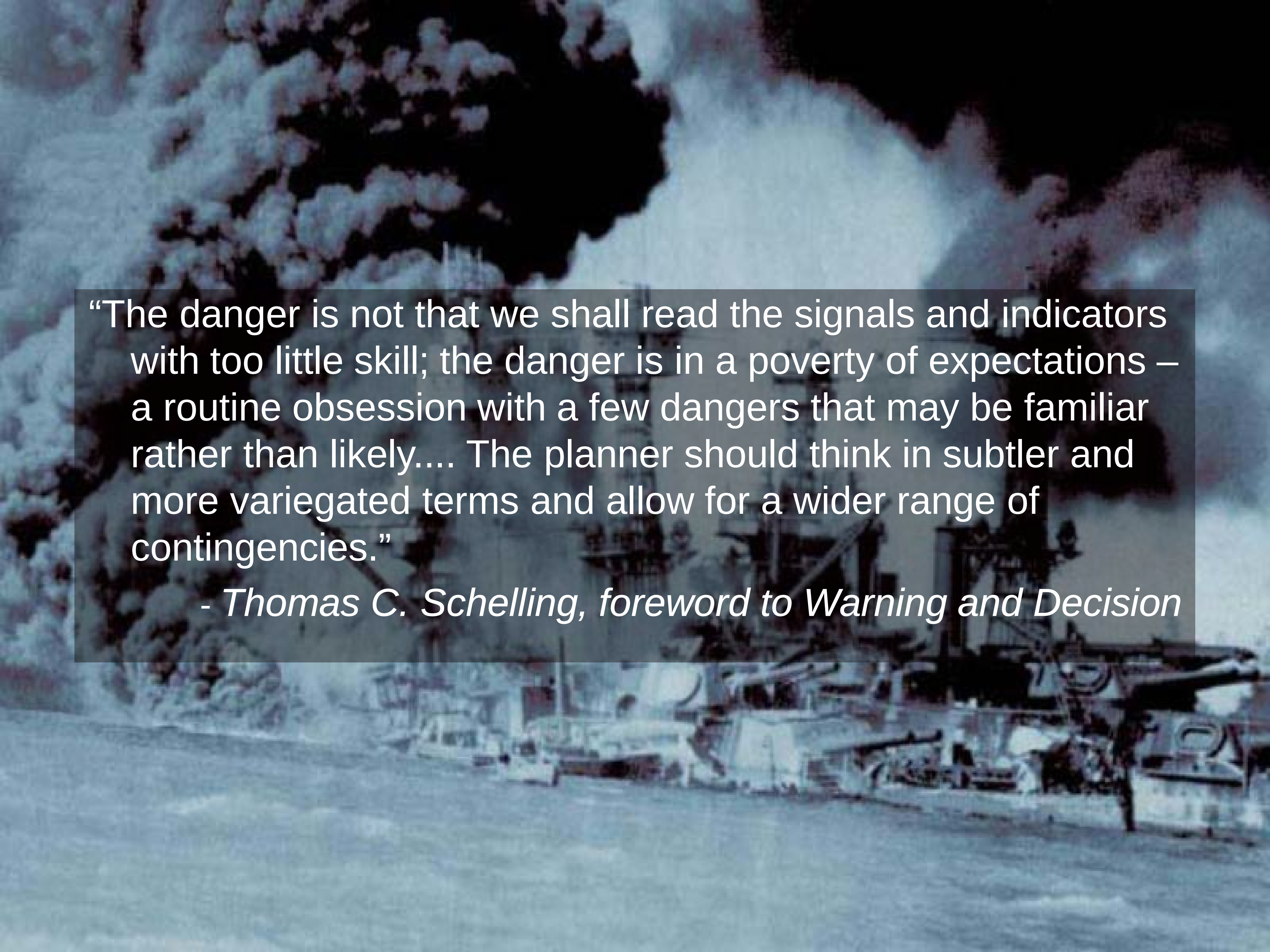
- The devil is in the digits!
  - Cyber attacks are a truly wicked challenge
    - Extent of the challenge growing in scale and dimensionality
    - Has capacity to augment virtually any other exploit
    - Insiders still the Achilles heel (now potentially unwitting)
  - A.I. is emerging gradually… until it’s all at once
    - A.I. could empower the adversary or become the adversary
  - Augmented and virtual reality also on the rise
    - Attack planning and rehearsal continually more realistic
  - Information ever more accessible and always dangerous in the right combination

Evolution of External Drivers (Tech.)

- Hardware is changing too
  - Additive manufacturing provides custom-built implements
  - Unmanned Aerial Systems
    - Scout, decoy or delivery vehicle
    - Precision drone swarming in the open source
  - Homemade chemical weapons
    - Precursors increasingly available
    - Criminal production (fentanyl)
    - DIY home labs improving

Technology for Defense

- Data integration and analytics
  - Put the puzzle together in time to preempt
  - Enhanced accounting and detection
  - A.I. to augment
- Virtual reality training for the defender
- Robotic sentries
  - Unblinking, unafraid and never forced from post
    - *But, potential new cyber vulnerabilities*
- New reactor designs and fuel handling
  - Less transportation, less refueling, less enrichment, less isotope separation, less volatility, more long-term storage



“The danger is not that we shall read the signals and indicators with too little skill; the danger is in a poverty of expectations – a routine obsession with a few dangers that may be familiar rather than likely.... The planner should think in subtler and more variegated terms and allow for a wider range of contingencies.”

- *Thomas C. Schelling, foreword to Warning and Decision*

Thank You

James Halverson
jhalvers@umd.edu
(301) 405-7131

www.start.umd.edu